<u>IN THE CLAIMS</u>:

Please amend the claims as shown below. The claims, as currently pending in the application, read as follows:

1. (Currently Amended) An inspection method for inspecting information stored in terminals that are included in a network, comprising the step of:

using a program module which moves between the terminals and determines, by using a public key digital watermarking method, whether a digital watermark is embedded in the information,

<u>wherein said public key digital watermarking method comprises decoding the information using error correction coding such that the embedded digital watermark is recovered from the information</u>.

2. (Original) The method according to claim 1, wherein when the program module determines that a digital watermark is embedded in the information, the information is downloaded from the terminal to an inspection server.

3. (Original) The method according to claim 1, wherein when the program module determines that the digital watermark is embedded in the information, the program module then checks, based on the digital watermark, if the user of the terminal is an authentic user of the information.

4. (Currently Amended) An inspection system comprising an inspection host for moving a program module, which determines, by using a public key digital watermarking method, whether a digital watermark is embedded in information stored in a terminal, between terminals that are included in a network,

wherein said public key digital watermarking method comprises decoding the information using error correction coding such that the embedded digital watermark is recovered from the information.

5. (Currently Amended) A computer readable recording medium that stores a program module which moves between terminals that are included in a network and determines, by using a public key digital watermarking method, whether a digital watermark is embedded in information stored in the terminal,

wherein said public key digital watermarking method comprises decoding the information using error correction coding such that the embedded digital watermark is recovered from the information.

6. (Currently Amended) An inspection method comprising:

a step of disclosing a part of digital watermark information related to a digital watermark extraction method on a network;

a step of installing at least the part of digital watermark information in a terminal which desires the installation of the digital watermark extraction method; and

an inspection step of inspecting authenticity of information in the terminal using the digital watermark information installed in the terminal,

wherein said digital watermark extraction method comprises decoding information using error correction coding such that the digital watermark information is recovered from the information.

7. (Original) The method according to claim 6, further comprising a step of informing, when illicit use of information is detected in the inspection step, a copyright protection terminal of the detection via the network.

8. (Currently Amended) An inspection method comprising:

a step of disclosing a part of digital watermark information related to a digital watermark extraction method on a network;

a step of licensing a terminal which is included in the network to use the digital watermark extraction method;

a step of installing at least the part of digital watermark information in another terminal via the use-licensed terminal; and

an inspection step of inspecting authenticity of information in the other terminal using the digital watermark extraction method installed in the other terminal,

wherein said digital watermark extraction method comprises decoding information using error correction coding such that the digital watermark information embedded in the information is recovered from the information.

9. (Original) The method according to claim 8, further comprising a step of informing, when illicit use of information is detected in the inspection step, a copyright protection terminal of that detection via the network from the other terminal.

10. (Currently Amended) An inspection system comprising a digital watermarking technique server which discloses a part of a digital watermark extraction technique on a network, and licenses a terminal which is included in the network to use the digital watermark extraction technique,

wherein said digital watermark extraction technique comprises decoding information using error correction coding such that a digital watermark information embedded in the information is recovered from the information.

11. (Currently Amended) An inspection method comprising:

an accept step of accepting a purchase application of information via a network;

a presentation step of presenting a copyright protecting technique used to protect a copyright of the information via the network;

a providing step of providing the information protected by the technique to a user when an agreement with the technique of the user who applied for purchase of the information is confirmed; and

an inspection step of inspecting authenticity of the information using the

technique by the user,

wherein said copyright protecting technique comprises decoding the

information using error correction coding such that a digital watermark information

embedded in the information is recovered from the information.

12. (Original) The method according to claim 11, wherein the presentation

step includes a step of presenting a measure to be taken against the user who illicitly used

the information.

13. (Original) The method according to claim 11, wherein the presentation

step includes a step of presenting to the user an extraction program which gives an

explanation about a digital watermark extraction method, and can inspect digital watermark

embedded in the information, and

the providing step includes a step of embedding, when identification

information of the user is confirmed together with the agreement, the user identification

information in the information as a digital watermark, and providing that information to the

user.

14. (Currently Amended) An inspection system comprising an information

vendor server which accepts a purchase application of information from a user via a

network, presents a copyright protecting technique used to protect a copyright of the

information to the user via the network, obtains a user's agreement for the technique as a

sales condition of the information, and provides the information protected by the copyright

protecting technique which makes it possible for the user to inspect authenticity of the

information, when the agreement is confirmed,

wherein said copyright protecting technique comprises decoding the

information using error correction coding such that a digital watermark information

embedded in the information is recovered from the information.

15. (Currently Amended) An inspection method comprising:

a storage medium providing step of providing a storage medium which

stores enciphered information embedded with storage medium identification information as

a digital watermark by using a public key digital watermarking method;

a presentation request step of requesting a user to present the storage

medium identification information and user identification information;

a providing step of providing a decipher program of the enciphered

information to the user in the presence of the presentation; and

an inspection step of inspecting authenticity of information by the user by

comparing the user identification information associated with the storage medium

identification information embedded as the digital watermark in the information, and user

information of a terminal that stores the information,

wherein said public key digital watermarking method comprises decoding the information using error correction coding such that the embedded digital watermark is recovered from the information.

16. (Currently Amended) An inspection system that sells enciphered information which is stored in a storage medium and is embedded with storage medium identification information as a digital watermark by using a public key digital watermarking method,

said system providing decipher software of the enciphered information to a user when the user presents the storage medium identification information and user identification information,

managing the storage medium identification information and user identification information in correspondence with each other, and

inspecting authenticity of information by the user by comparing the user identification information associated with the storage medium identification information embedded as the digital watermark in the information, and user information of a terminal that stores the information,

wherein said public key digital watermarking method comprises decoding the information using error correction coding such that the embedded digital watermark is recovered from the information.